April 1990/Number 3-90

security awareness bulletin

Inside:

Special Edition

Department of Defense Security Institute, Richmond, Virginia

security awareness bulletin

Approved for open publication Unlimited reproduction authorized

Director
Department of Defense Security Institute
R. Everett Gravelle

Editor
Lynn Fischer

Staff Writer
Tracy Gulledge

The *Security Awareness Bulletin* is produced by the Department of Defense Security Institute, Security Education and Awareness Team, 8000 Jefferson Davis Hwy, Bldg 33E, Richmond VA 23297-5091; (804) 279-5314, DSN 695-5314. Fax: (804) 279-5239 or DSN 695-5239. Primary distribution is to DoD components and contractors cleared for classified access under the Defense Industrial Security Program and Special Access Programs. Our purpose is to promote security awareness and compliance with security procedures through dissemination of information to security trainers regarding current security and counterintelligence developments, training aids, and educational methods as well as through distribution of textual material for direct training application.

Administrative inquiries, new distribution, address changes: please refer as follows:

Army activities: HQ DA (DAMI-CIS), Washington, DC 20310, (703) 695-8920, DSN 225-8920;
POC Jim McElroy

Navy & Marine Corps: Security Policy Div (OP-09N), Washington, DC 20350 (202) 433-8858, DSN 288-8858;
POC Sue Jones

Air Force: Headquarters AFSPA/SPIB, 8201 H St SE, Kirtland AFB, NM 87117-5664, DSN 246-4787;
POC Ken Saxon

DIS activities: HQ DIS/V0951, 1340 Braddock Place, Alexandria VA 22314-1651

DISP contractors: Cognizant Security Office

Other government agencies: Headquarters security education office

An Introduction to Beyond Compliance

This edition of the *Security Awareness Bulletin* is devoted almost exclusively to a recent report by PERSEREC, the Defense Personnel Security Research and Education Center in Monterey, California. Although the result of extensive interviewing and first-hand observation, "Beyond Compliance" is not a research report in the conventional sense. It is in fact a very effective management handbook, having a firm grounding in reality. The authors share with us in a readable and entertaining way what has worked well in defense industry, how some Facility Security Officers have been uniquely successful, and how these initiatives mesh with contemporary management literature.

Although most of the discussion is keyed to security professionals in industry and to the requirements of the Defense Industrial Security Program, the practices easily translate to security programs within the Department of Defense and in other Federal agencies. There are some universal principles described here which echo many of the ideas in Joe Grau's much admired article on "Selling Security" in the May 1989 *Bulletin*. I think you'll enjoy "Beyond Compliance," and I hope it inspires you to try some different approaches that may help you improve your organization's effectiveness as you continue to protect the Nation's secrets.

R. Everett Gravelle, Director
Department of Defense Security Institute

PERS-SR-90-001 MARCH 1990

BEYOND COMPLIANCE: ACHIEVING EXCELLENCE IN DEFENSE INDUSTRIAL SECURITY

Ernest V. Haag
HumRRO International, Inc.

Kent S. Crawford
James A. Riedel
Suzanne Wood
Defense Personnel Security Research
and Education Center

Connie J. Schroyer
HumRRO International, Inc.

Released by
Roger P. Denk
Director

Defense Personnel Security Research and Education Center
Monterey, California 93940-2481

TABLE OF CONTENTS

TABLE OF CONTENTS

FOREWORD

Within the Defense Industrial Security Program, there is considerable information available on security requirements. Unfortunately, there is only limited guidance to help security professionals translate these requirements into effective security programs. Recognizing this deficiency, PERSEREC undertook this study.

Rather than concentrate our efforts on what was not working, we looked at the high side of security--how effective security programs were being managed. Much can be gained by focusing on excellence rather than on deficiencies. If we could capture ideas and approaches that worked well for effective facility security officers (FSOs), other FSOs could then use these to improve their own security operations. Our objective was to record what effective FSOs told us and present this information in a manner that will enable other FSOs to incorporate some of the ideas into their own programs. We chose an informal style of presentation since we wanted to convey our findings in the language of our primary audience, the FSO. Government security managers may also find information in this report useful since they face many of the same management challenges as their counterparts in defense industry.

The authors would like to thank the numerous individuals who assisted in conducting this study. First, at Defense Investigative Service (DIS) headquarters, Bob Schwalls, Deputy Director (Industrial Security), provided both strong support and encouragement for this project. Without his assistance, we would not have been able to complete the project. Each of the Cognizant Security Office Directors of Industrial Security willingly participated in interviews and allowed us to spend time talking with their staffs. Also Ev Gravelle, Joe Grau, and the industrial security staff at the Defense Security Institute shared their ideas. On the industrial side, two individuals merit special thanks: Larry Howe of Science Applications International Corporation and Dick Black of SRI International. Early discussions with them provided us with a general model of security effectiveness that was critical for developing the interview protocol and for interpreting the data. Finally, we would like to thank the FSOs who participated in this study. We trust that this report has done justice to the numerous ideas that they shared with us during our visits to their organizations.

The report is organized into five chapters. The heart of the report is chapters II through IV. Each of these chapters can be read independently, allowing the reader to choose only topics of particular interest. This report will be valuable to new FSOs and to DIS personnel who work with FSOs and inspect their security programs. It should allow the DIS Industrial Security Representatives to see what their counterparts in industry are attempting to accomplish on a daily basis.

The last page of this document is a brief evaluation form. We would appreciate your feedback on the usefulness of the information in this report.

ROGER P. DENK
Director

BEYOND COMPLIANCE: ACHIEVING EXCELLENCE IN DEFENSE INDUSTRIAL SECURITY

Chapter I

INTRODUCTION

More inclined to guarding against malfeasance than to encouraging excellence, we have overlooked the obvious.

- Jay Hall, The Competence Connection: A Blueprint for Excellence.

The Defense Industrial Security Program (DISP) was established to ensure that classified information released to industry is properly safeguarded. It encompasses approximately 12,000 contractor organizations and 900,000 cleared employees. With regard to the protection of classified government information, the heart of the DISP is the security program in place at each of the contractor sites.

Facility security officers (FSOs) play a key role in translating Department of Defense (DoD) security requirements into organization-specific Standard Practice Procedures that serve as the security manuals for defense contractor sites. FSOs are tasked with implementing and maintaining security programs that meet DoD security requirements as presented in the DoD 5220.22-M, Industrial Security Manual for Safeguarding Classified Information (ISM). However, rules and procedures alone do not guarantee acceptance and compliance by cleared employees. FSOs must ensure commitment to security requirements through support from management and other key groups, and through security education and training programs. FSOs must be effective managers if their programs are going to be successful.

Given the size and complexity of the DISP, it is not surprising to find varying levels of security effectiveness at the different contractor sites. Inspections by the Defense Investigative Service (DIS) are reminders that some FSOs are more successful than others. To date, however, there have been no systematic studies examining management excellence in the DISP. We wanted to look at what highly effective FSOs were doing on the job. For example, what types of management practices were the more effective FSOs using; how were they acquiring top management support for their security programs; and how were they were gaining commitment from employees for following security requirements?

OBJECTIVES

By interviewing effective FSOs, we wanted to document their management practices. We accepted the premise that there are many ways to achieve an effective security program. But we also believed that certain management approaches worked better than others in certain organizational settings. The overall aim was to present the findings in a manner that would be useful for FSOs, the audience for this report.

This study had four objectives. The first was to describe the management practices of superior FSOs. By identifying FSOs who have reached a consistently high level of security performance in their companies, we wanted to focus our attention on the high side of security management, to get away from looking for what is wrong, and zero in on what is right. By their performance, these FSOs have gained recognition within the security community and have been a positive influence on their immediate circle of associates.

The second objective was to stimulate thinking in the industrial security community about what constitutes excellence and how it can be achieved. Given the large number of government contractor organizations involved in classified work, the potential benefits from program improvements are significant. Even small improvements in management effectiveness, spread over that many security programs, can ultimately make a real difference in both the efficiency and effectiveness of a large, complex system.

The next objective was to provide guidelines for the professional development of government security managers by developing a model of an effective FSO. There may be those, perhaps new to the security world, who only need a better defined standard to take their own programs to higher levels of excellence.

Our last objective was to provide recognition for a large community of professionals who face special challenges in their work place. The FSO must serve two demanding masters. One is the DIS representative, the inspector who must ensure that the FSO and the organization are complying with the security requirements of the ISM. The other is management personnel within the organization who are constantly seeking improved efficiency and effectiveness and who may sometimes question the value of the security department's contributions to these goals. The FSOs described in this report have not only met these challenges, but have on balance surpassed the standards which have been set for them.

RESEARCH PERSPECTIVE

Recent research in the area of management and leadership has led many managers to shift their perspective towards excellence when considering issues of organizational effectiveness. Until the last decade, most management training focused on developing skills for identifying and solving problems. Little formal attention was paid to developing a model of the positive side of management and proactively using it to guide management thinking and behavior in the marketplace.

Tom Peters and Robert Waterman (1982) were among the first authors in the 1980s to articulate the new perspective in a way that gained widespread public acceptance. It is fair to say that their book, *In Search of Excellence*, has revolutionized the way many managers assess their organizations and their employees. Likewise, in *The Competence Connection*, Jay Hall (1988) reinforced Peters and Waterman when he stated, "More inclined to guarding against malfeasance than to encouraging excellence, we have overlooked the obvious" (p.29). These authors have given us their model for excellence and ways of analyzing its foundations which have broad applicability in a number of work environments.

The terms which they invented (e.g., management by walking around (MBWA), close to the customer, bias for action, a presumption of competence, etc.) are widely used in the business world. Many managers use them to describe what they are trying to accomplish in their own environments. The concepts behind the words have become the standards by which managers now try to assess their organization's performance and their own contributions to organizational excellence. It is no different among government FSOs in industry.

APPROACH

Selection of facilities. The field research was confined to Class A or B facilities. Although these facilities constitute less than 4 percent of

the total number of organizations in the DISP, their size ensures that they perform a large proportion of the classified work. It was decided that the range of issues faced, the complexity created by size, and the multiplicity of classified contracts in the larger organizations would give us a rich body of data.

The sample of FSOs was nominated by DIS as representing top security performers within their region. Nominations were based on a number of criteria. The most important were:

1. The security program is well managed. The FSO shows initiative and creativity in meeting or exceeding ISM requirements.

2. The security program at the facility has been consistently outstanding (or showing major annual improvements) over the last two to three years. The FSO may or may not have won a Cogswell award for any particular year; however, the security program is consistently one of the best in the region.

3. The results from DIS security inspections at the facility over the last two to three years have exceeded the average marks achieved by other facilities in the region.

Nominations were received that provided a selection of FSOs representing geographic regions and a wide variety of business types. A near equal sample was selected from each of the eight DIS regions.

Selected FSOs nominated other FSOs who had excellent security programs. Based on input from both the DIS regions and the FSOs, we identified the final sample of 36. There was considerable agreement between the nominations of DIS and those of the effective FSOs. Twenty-four of our interviewees were nominated by both the DIS regions and the FSOs whereas the remaining 12 were divided between FSO-only and DIS-only nominees. By the end of the study, three or more FSOs in each of the eight DIS regions had been interviewed. A total of 36 contractor organizations in the DISP were visited. We obtained approximately 120 hours of taped interviews, spending from 3-8 hours at each of the facilities visited. It should be noted not every FSO nominated by DIS or other FSOs was interviewed; there were more nominations than we had time or resources to contact.

Also included in the sample were the DIS Industrial Security Directors from each of the eight DIS regions. Their extensive experience in inspecting contractor security programs provided a valuable perspective on what constituted security excellence.

Interview process. The interviews covered three areas: the management practices of effective FSOs; how FSOs went about gaining support from key groups such as top management, the security staff, DIS, the customer, and professional colleagues; and how the FSOs developed and implemented their security education and training programs.

MOVING BEYOND COMPLIANCE

The overall findings are presented first. These provide a framework for organizing and interpreting the specific findings presented in the remaining chapters.

During the interviews, we seldom heard the word *compliance*. FSOs knew they must be in compliance with the ISM, but they saw this as a natural result of working towards their primary objective: having the most effective and efficient security program possible.

Asked about primary goals, a large majority gave responses like, "Being the most effective security operation" or "winning the Cogswell Award." The FSOs viewed compliance as a minimum performance standard. They achieved compliance by pursuing excellence.

They were especially creative when it came to deciding how to achieve excellence. FSOs described practices such as prescreening all new

hires for potential security clearance eligibility, conducting security briefings for noncleared employees, and automating various record-keeping and documentation processes. We were also told of many innovative practices in security education and awareness training programs and numerous ideas for better integrating security with other functional areas of the company. All were actions taken in the name of doing more with less. These FSOs wanted more than just a "check in the box" for compliance. They wanted the satisfaction that comes with setting higher standards and achieving them, of being recognized by their peers for accomplishments, and making a positive contribution.

Going beyond compliance did not mean gold-plating. It meant continually seeking ways to improve security programs. It meant understanding the needs of their diverse customers--DIS, project managers, employees, top management, and the contracting agency. In essence, going beyond compliance was the process of being proactive rather than reactive, and getting people involved in the security program in order to create workable security rules and procedures. It was seeking excellence by being a leader for security. The result was a security program that was both cost-efficient and requirement-effective.

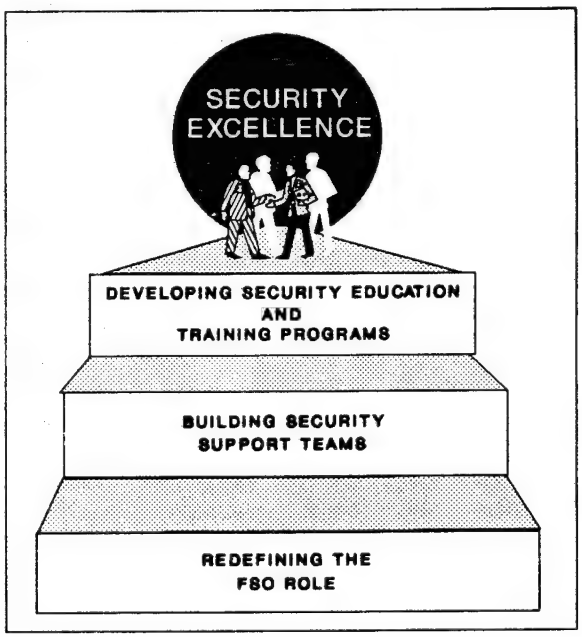
What, then, were the key areas where the FSOs moved beyond compliance and achieved security excellence? First, FSOs redefined the traditional role requirements of the security officer. Second, they built security teams that provided the key support necessary to implement and maintain their programs. Finally, they gained the commitment of employees to effective security through a security education program that stressed employee involvement. Each of these areas is discussed in greater detail in the chapters ahead.

THE COMMON THEME: SELLING SECURITY

There is one theme linking the three areas--the need to sell security. The FSOs did not assume that management and employees would automatically support security program objectives. These FSOs sold security. In an article in the *Security Awareness Bulletin*, Joseph Grau (1989) has described the use of marketing techniques to get people to accept the security program. His discussion of security as a service industry complements the comments of our FSOs. As Grau noted:

> If one of our key responsibilities is to get people to "buy into" our security program, then we're going to have to *sell* it to them. And if we're going to do this effectively, I think we need to step back for a moment and take a good look at what our role in our organization really is (p. 1).

The basic framework around which the rest of this report is organized has been presented. The next chapter will present more detail on the initial step in the beyond compliance model--redefining the FSO role. As Grau has recommended, we take a new look at the role of an FSO.



Chapter II

REDEFINING THE FSO ROLE

"In this company, if the project engineer doesn't know who I am, security is in trouble."

The traditional role for an FSO is that of the company security officer. He or she makes sure that security rules are understood and enforced. The FSO has organizational authority, and fear of punishment is the primary motivator for employee compliance. This role is important; however, it is only the beginning. It does not guarantee compliance, let alone go beyond compliance. Employee resistance to security procedures may develop, and management may not provide the support necessary for effective implementation of the security program.

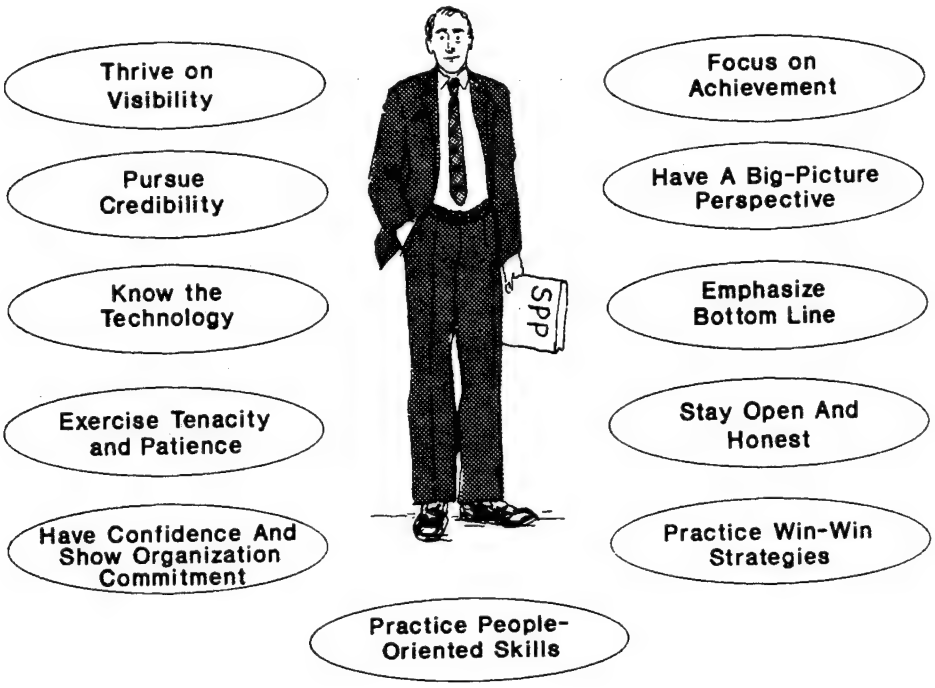
There were 11 strategies that effective FSOs used to expand their role. While the FSOs may emphasize different strategies depending upon unique organizational requirements, the 11 strategies represent a composite description. They are management practices that provide the FSO with the capability to be a catalyst for proactive change.

THRIVE ON VISIBILITY

The FSOs repeatedly stressed the importance of being visible to everyone in the company, from top to bottom. Visibility to those in top management, including the president, was cited as a key element in the ability of the FSO to gain and maintain support for the security program. In a moderately sized electronics company, one FSO said, "In this company, if the project engineer doesn't know who I am, security is in trouble. I don't like to see my staff sit too long at their desks. They can do more good for security and the image of this department out on the floor, talking to the guys who do the work than they can by finishing a piece of paperwork." Exercising security by walking around (SBWA) and being recognized as a security professional were important ways to make security visible.

These FSOs wanted to set an example for their security staff by making themselves available to others in the organization. They wanted to be seen doing their job, helping others to understand and accept security as an integral part of the organization.

The FSOs reported that they expend a great deal of effort building and continually adding to their network of contacts within the company. They make an effort to drop in on the project managers, the newer ones as well as the top management level (vice presidents and directors), to find out if there are any security issues that need to be clarified. They emphasize the idea that security is there to solve problems, not make them. Moreover, they pay particular attention to the decision-makers who have an impact on the destiny of the security function. "It may be office politics," said one, "but when I have an urgent security need, I want the top management to know me as someone other than just another middle manager with a problem."



Appearance was another aspect of visibility. The image of security starts with the behavior of the security staff, and includes their personal appearance and that of their work space. The location of the security office is also important. Many FSOs stressed that their offices need to be located in convenient places.

In one company, the security office has a comfortable seating area and a pot of coffee for the drop-in visitor. What started as a courtesy to fellow employees has become essential for spreading the security gospel throughout the company via the informal conversations that take place in the security office. This may sound like SBWA in reverse, but it works. The key, of course, is that the security office must be seen as a place where problems get solved, and assistance is professionally and cheerfully provided.

PURSUE CREDIBILITY

It was felt that SBWA gives the FSO opportunities for positive influence and can only enhance credibility. But it does nothing to create it. One FSO said that credibility is "...simply my lifeblood. If I don't have it, if my people don't have it, we're dead." The FSOs believed that being credible includes the ability to discuss security requirements in a professional manner. Credibility also depends upon whether the FSO inspires confidence, invokes trust in others, and represents security in ways that fit the organization's culture.

The importance of fitting into the facility's culture as a means of creating credibility can be illustrated by our observations at two organizations. One, a highly structured and hierarchical organization, seemed to live literally by the book. The organization was described as very paternalistic. The FSO had been with the company for more than 12 years and had been brought in to solve security problems. He was a near perfect reflection of the culture in which he worked. Dynamic, aggressive and authoritative, he was clearly a visible and credible security presence wherever he went in the large facility.

He explained that those were the styles that had made him successful and, "...besides, the top management is a lot like that, so it must be OK."

The second organization was a moderate-sized technical research company with a majority of its staff composed of research scientists. The culture was very different: quiet as opposed to bustling, relaxed rather than hyperactive. The FSO was a perfect match. An effective professional, soft-spoken and unhurried, she also gave the impression of competence. It became obvious that her style was much less directive, and more collaborative and persuasive.

These examples show how both FSOs communicated with top management in ways that successfully sold security issues. The reason they were so successful is that they have adapted to doing things in ways that were consistent with their particular corporate culture.

When asked for examples of successful efforts to gain support for security needs, some FSOs reported instances where success had followed an unsuccessful period. The transition seemed to come always after a shift in approach which brought the FSO into better alignment with "the way things are done here." In each of these cases, better meshing with the culture brought about acceptance of the FSO's position, as well as an improved perception of the security department and the professional credibility of the FSO.

When asked how he developed and maintained his own credibility, one FSO said, "I've got to have the answer to their questions. If I don't, I've got to find someone who does."

Showing an understanding of the problems faced by project managers (and not just in the security realm) is another way several FSOs reported they were effective in achieving credibility. It seemed that being able to place security issues in the context of the project manager's overall concerns lent credibility to the FSO.

Another FSO talked about gaining credibility with top management by knowing their chief concerns. "It always helps," she said, "if I know and am able to talk about the financial impact of some new security requirement that we or the government have come up with." Her company was going through a period of retrenchment, and financial performance was especially important.

Being responsive to management concerns helps to build credibility. FSOs must stay on top of changing conditions. How quickly the security department responds to crises or even minor problems; how the guard force interacts with employees; the personal appearance of security staff; the quality of paperwork from the security department--all were reported to have an impact on credibility. One company placed great emphasis on thorough staffing of issues. The FSO said that "...the best way to create credibility is to make sure that when I take an issue up for a decision, all alternatives are included and analyzed, and I know what the best solution is. All I want is approval of my recommendation."

Building credibility was also very closely related to trust. "Never lie or give a mealy-mouthed answer." "Always be straight." "Don't try to cover up your mistakes." "Show you're a team-player." "Give a lot of credit to others." "Don't be the company cop." "Give consistently accurate answers." The FSOs seemed to be achieving credibility in three ways: (1) knowing the security requirements, (2) working professionally with others, and (3) understanding the company's business and how security played an important role in the company's success.

Trust and confidence are the building blocks of credibility. One FSO said that because of personal interest and background he had gradually established a reputation as a willing counselor for people with both personal and professional problems not associated with his security role. As a result, he reported an increase in the number of people coming to him with security concerns--not only those he had counseled, but others as well. He attributed this to the personal trust and

confidence of others that he had acquired through his counseling efforts and through the company's informal communications networks which passed the word that he was honest, straightforward and willing to help.

KNOW THE TECHNOLOGY

We found that FSOs understood the technical side of their company's business. They could communicate with top management and project managers about technical requirements for security with an understanding of the impact security would have on all company activities.

As one FSO stated, "I have been with the company practically since it started. I know all the methods of production. I could probably do the job of a lot of the project managers. But my best contribution is that I know how to mesh security with production in ways that don't negatively affect production." Another advantage of his experience with the technology was that the company's customers knew the value of his knowledge and that he seldom had difficulty meeting their requirements. In fact, the customers frequently came to him for security advice.

Knowing the technology enabled FSOs to determine when a Request for Proposal (RFP) would create security problems which needed to be considered in putting together a bid. They felt such knowledge can be invaluable to the organization. The FSO is familiar enough with ongoing work to know when classified facilities are under- or over-utilized, and what additional security investments will have to be made to meet customer requirements. The FSO also knows how many different levels of cleared personnel are required for a particular work process and can make a real contribution to the team charged with putting together a competitive bid.

Being knowledgeable about the work place and being able to converse intelligently with the employees about their work can also lend additional credibility and trust to the FSO. An FSO in a large electronics manufacturing firm said, "I accomplish more security education on 'walk arounds' because I am interested in how the employee does the job and I ask intelligent questions. I can also see security problems that the employee may not be aware of."

EXERCISE TENACITY AND PATIENCE

Effective FSOs take a long-range view of their program and develop strategies for achieving objectives. One mentioned that he had been trying for 3 years to become a member of the team which considers whether a response will be made to an RFP. After trying numerous strategies to insert himself into the process, all of which failed to some degree, he finally succeeded by taking a more direct route--an analysis of the cost-benefit of his participation.

This illustrated the FSO's determination to succeed. He might well have been discouraged by repeated failure to gain acceptance. Instead, what he learned provided not only the impetus for trying again, but also pointed him in the direction of the final strategy, the one that would work. Our interviews were filled with statements about "finally making it happen."

Being patient with failure often led to eventual success. In many cases, doing the homework necessary for getting through to top management, sometimes over and over again, was critical. When asked for the key to her success, one FSO paraphrased a popular advertising slogan, "We got a successful security program the old fashioned way: we worked damned hard for it!"

HAVE CONFIDENCE AND SHOW ORGANIZATION COMMITMENT

FSOs recognize that they are the experts in their field, and they freely exercise their expertise. They are highly experienced and have solved many problems during their careers. They averaged 18 years of experience in government security. That does not include years of experience prior to

joining the industry as members of the armed forces or other government agencies.

McClelland and Burnham (1976, pp.105-106) describe four major characteristics of the institutional manager that seem to fit our FSOs:

1. "They are more organization-minded."

FSOs joined more organizations and felt responsible for building them up. Most were active members, even officers, in various security organizations, and many contributed their time and talents to other organizations outside their work environment.

2. "They report they like to work."

FSOs actually seemed to like the discipline of work and enjoyed being a part of the security business. It satisfied their need to get things done in an orderly way.

3. "They seem quite willing to sacrifice some of their own self-interest for the welfare of the organization they serve."

FSOs spoke of their job in terms of assisting and supporting. One particularly energetic FSO reported, "I often start thinking about the job when I wake up in the morning and sometimes stop thinking about it when I go to bed at night." Giving their energy and concentration to the job was a common theme.

4. "They have a keen sense of justice."

These managers felt that if people work hard and sacrifice for the good of the organization, they will get a just reward. The FSOs seemed to have their own way of recognizing performance in their own staff as well as in others with security responsibilities in the organization. One stated, "The company has a very good and fair merit system, but I have to augment that with a personal touch, a pat-on-the-back, a *well done*! or a handshake. This is what makes a difference to people." The FSOs thought a lot about how they could reward their people for hard work or innovative behavior, realizing that a successful security effort required a great deal of both.

FOCUS ON ACHIEVEMENT

Proactive rather than reactive change was continually emphasized. The FSOs had a vision of what they wanted to accomplish. They continually focused on achievement. Here, another of McClelland's research findings is relevant: the need for achievement as a motivating force. McClelland and Burnham (1976) define the need for achievement as "...the desire to do something better or more efficiently than it has been done before" (p. 100). Almost every FSO looked for a better way to do things and expressed a desire to have the best program possible. These are classic indications of the way achievers think and operate.

Achievers also set objectives for themselves and others. Most FSOs had a clear picture of where their department was going and a plan for getting there, even in those companies which did not have a formal goal-setting system. Like the manager who is strongly motivated to use his or her power for the benefit of the organization, the individual who has a high motivation to achieve also tends to enjoy being a mentor for others.

The FSOs' focus on achievement can be seen in their positive approach to problem-solving. When an FSO was asked how she gained management support for solving security problems, she replied, "We don't have security problems (here)--only challenges." She made a concerted effort to view problems as challenges because, as she intuitively knew, people tend to respond more positively to challenges than to problems. In summary, it was clear to us that the FSOs were highly motivated by need for achievement.

HAVE A BIG-PICTURE PERSPECTIVE

Effective FSOs had a macro view of their world. They made it a priority to stay informed about what was happening in the government

security field and in their own industry. In addition to handling the day-to-day problems of any middle management job, they had a broader perspective. Several FSOs spoke of taking some time during the day to ponder both internal and external security events and their likely impact on themselves and their company.

In order to see the full range of options which most issues generate, FSOs need to consider the implications and effects of actions on other parts of the organization. They need to consider not only those actions initiated within the company, but also those originating from external sources (e.g., government, the competition, etc.). This is not only good management, it is good politics. It allows the FSO to be better informed of possible complications that may be important to top management. The FSOs quite often spoke of being able to communicate to their staff and superiors the possible effects of security program changes on their ways of doing business.

They maintained affiliation with an active network of contacts in both government and industry, so that they stayed informed about potential changes, new ways of operating, and new technology applications. One stated, "It's not easy to stay actively involved with outside contacts, with all the many daily demands and problems you have to deal with, but I have to pay that price in order to do the best job I can, and besides, I enjoy it." Not only was this good for their own interests, but the knowledge gained paid additional dividends when information was passed on to staff and top management. The result was improved professional development of subordinates and sometimes significant insights to solving security problems.

FSOs gained by staying abreast of job-related developments, and they also helped others by sharing this knowledge and experience. By keeping project managers informed of potential security problems, FSOs contributed to the managers' ability to work effectively at accomplishing project objectives.

EMPHASIZE BOTTOM LINE

Translating security objectives into economic terms was important. Most chief executives are extremely cost-conscious and demand that their managers plan budgets carefully, execute spending in accordance with their plan, and justify unplanned expenditures. The FSOs are more effective if they can understand and speak the language of the financial decision-makers. In companies with high emphasis on bottom-line economics, it is important to make that a key part of security thinking.

FSOs are always thinking of ways to economize and still get the job done effectively. They try to document financial impact to improve credibility with top management. One stressed that the FSO cannot always obtain necessary approval for security changes based on the fact that "...regulations (or the customer) require it." He said, "I always figure out what a security change is going to cost and whether there are less costly alternatives that will achieve the same result." He also checks his ideas with his customers for other alternatives and then goes to the decision-maker with the whole package. "It's hard to argue with success," he said. "I've never been turned down when I've done my homework and can lay out the figures."

One FSO makes sure that any savings from improved security procedures are reported in his periodic briefings to top management. This attention to the financial impact of the security program sends a message to top management that the FSO is concerned about the financial performance of the company.

STAY OPEN AND HONEST

The importance of openness and honesty was stressed time and time again. For example, when one FSO realized the importance of financial analysis to the top management of his company and that his own skills in that area were weak, he went to an expert for help. He found an individual in the financial office with the skills he

sought and an interest in helping. After explaining his concerns about his own ability and his ideas as to what level of financial analysis was needed in the security department, he got more help than he had envisioned.

His financial mentor made recommendations regarding what things might be financially quantified and tracked and how to conduct rudimentary cost-benefit analysis, as well as suggesting ways to present data clearly and in the form preferred by top management. All this resulted from simply being honest about his limitations. In this case, the FSO not only was able to improve his own professional skill level but he also enhanced his credibility with the financial office.

FSOs advocated sharing information with others. Many described instances where they had resolved situations of their own by referring to solutions learned from others. They also spoke of their sense of obligation to let others know when they had found solutions to particularly thorny problems. They all seemed to say, "There should be no secrets in security management. We all learn more by sharing ideas and solutions."

All were positive about the value of being candid with DIS representatives. They reported uniformly excellent relationships with DIS, seeing the representatives as a primary resource for resolving issues and getting necessary information. Being honest with DIS representatives, reporting recognized security shortcomings, and asking for their assistance had almost always paid off. Not only were the relationships strengthened, but their own effectiveness was usually enhanced. Such willingness to take a risk with openness built trust and helped create a better team environment.

PRACTICE WIN-WIN STRATEGIES

The FSO's basic approach to resolving interpersonal conflict could be summed up as *win-win*. That is, both parties gain something from resolving conflict rather than one party winning and the other losing. The FSOs usually set as a high priority being well informed about any conflict. They expressed a desire to understand the issues and the people involved before attempting to confront the other party or intervene between parties. Knowing what interests would be served by what outcomes and having a clear picture of the circumstances surrounding the conflict were basic to reaching a win-win resolution.

One FSO approaches conflict by analyzing each possible solution for its impact on the involved parties. The trick is to find the solution that results in positive outcomes for all; in some cases this many mean minimizing the negatives. His point was that in a conflict situation, especially one involving the FSO, shooting from the hip is never the best approach. FSOs should ask: "Is there any solution that will allow all parties to get most of what they want?" and "How can I best influence that outcome?"

Another FSO reported that one of the main values of the win-win approach is that it sets an example for constructively resolving conflict. One problem with entering a conflict situation with a

win-lose attitude is the assumption that the other party is thinking the same way, and that the only way to survive is to fight harder for the outcomes you want. Operating from a win-win stance may create the first realization by the other party that there need not be a loser.

PRACTICE PEOPLE-ORIENTED SKILLS

The last strategy is one that permeates most of the other 10 and is also critical to the ideas discussed in the remaining chapters of this report. When asked to describe their own approach to their job, FSOs tended to speak in terms more often associated with leadership than management--influencing behaviors, facilitating achievement by subordinates, developing skills in others, setting a personal example, and mentoring.

One FSO described how effectiveness was improved through interpersonal style. "I believe I am a better manager when I *pull* my people to achieve, not push them." Pushing was a term used to indicate managing by direction, while pulling referred to leading by example. This FSO felt that most people do better when they get a chance to lead once in a while. A strong leader provides the example, then encourages subordinates to demonstrate their own initiative and ability. Another FSO put it this way. "I believe my people are better off when they manage themselves. If I can show them the way and help them to be better managers themselves, I am better off as well."

In their best-selling book, *Leaders*, Bennis and Nanus (1985, pp. 66-67) cited the five key interpersonal skills used by 90 outstanding business leaders.

1. "The ability to accept people as they are, not as one would like them to be."

This skill was evident in the approach FSOs took to staff development. Almost all talked about building the skill they needed in their staff, not looking for a ready-made security expert. They openly recognized that the best people do not always shine when first discovered. They often reported hearing about people who might be good for security, then observing them at work, asking their supervisors about them, and assessing their potential.

They did not often turn people down simply because they lacked the technical skills of a security professional. Rather, they looked for interpersonal skills on which they could help individuals build security expertise. This orientation was even more evident when the FSOs described how they influenced their peers and top management. As one said, "You have to find out who they are, what they are like as a person, what their pet peeves are--and then, you've got to get in sync with them."

2. "The capacity to approach relationships and problems in terms of the present rather than the past."

A common theme was that every day was a challenge. There was not time to dwell on the past. The central idea was: learn from what has happened and move on. Many told us that they examine every situation in terms of current conditions and resolve problems from that perspective. What was an overriding concern of the executive vice-president last week and the basis for approaching him then may not even be on his mind today.

3. "The ability to treat those who are close to you with the same courteous attention that you extend to strangers and casual acquaintances."

Courtesy and friendliness toward subordinates and coworkers was certainly the norm. The FSOs valued their relationships with others. In most organizations we found a collegial environment with collaborative relationships. The atmosphere was businesslike and professional, yet friendly.

Bennis and Nanus report that sometimes in organizations we become so familiar with the people and their work that complacency obscures our sensitivity to what is going on. We may lose

our ability to listen to what people are saying or to appreciate the quality of their work. In this case everyone loses. Selective listening, Bennis and Nanus suggest, may lead to misunderstandings. Insensitivity also restricts our ability to give feedback and demonstrate our attentiveness and concern.

4. "The ability to trust others, even if the risk seems great."

Building trust was an important duty. Said one FSO, "I've got to prove to my people that I trust them, and that they can trust me. I try to pick good people, pay and train them right, give them direction and then turn them loose." Equally important was the need to build a bond of trust with both project managers and top management.

As Bennis and Nanus (p. 67) state, "A withholding of trust is often necessary for self-protection. But the price is too high if it means always being on guard, constantly suspicious of others. Even an overdose of trust that at times involves the risk of being deceived or disappointed is wiser in the long run than taking it for granted that most people are incompetent or insincere."

5. "The ability to do without constant approval and recognition from others."

Effective leaders tend to be inner-driven, see rewards in the work itself, and have their own standards to meet. Having a high need for approval can cause problems. Because it is in the nature of their work to take risks, leaders should be ready for occasional disharmony and dislike. Risks cannot be a pleasure for everyone. When speaking of their personal achievements, most of the FSOs emphasized circumstances where the results came from taking initiative and influencing a team or group effort. They often talked of placing themselves at risk by taking a strong stand or by making innovative changes. Whatever their approach, it was clear that these FSOs were much more inclined to take the lead than to wait for someone else to follow.

SUMMARY

We have identified and described 11 strategies used by effective FSOs to redefine their role. This is the first step in moving beyond compliance. In the next chapter, we turn to the role of security support teams in providing assistance to the FSO in implementing and maintaining an effective security program. The strategies discussed in this chapter serve as a foundation for developing these teams.

CHAPTER III

BUILDING SECURITY SUPPORT TEAMS

Sowing seeds of trust with people creates the fields of collaboration necessary to get extraordinary things done in organizations.

- James Kouzes and Barry Posner,
The Leadership Challenge: How to Get Extraordinary Things Done in Organizations.

No matter how much they have expanded their role, FSOs cannot implement and maintain an effective security program without developing support from key groups. This means building and maintaining security teams that serve as the supporting cast. Support from these groups depends on creating a collaborative working climate. First, we will focus on how FSOs foster such a climate and then how they use that climate to help build the support teams.

CREATE A COLLABORATIVE CLIMATE

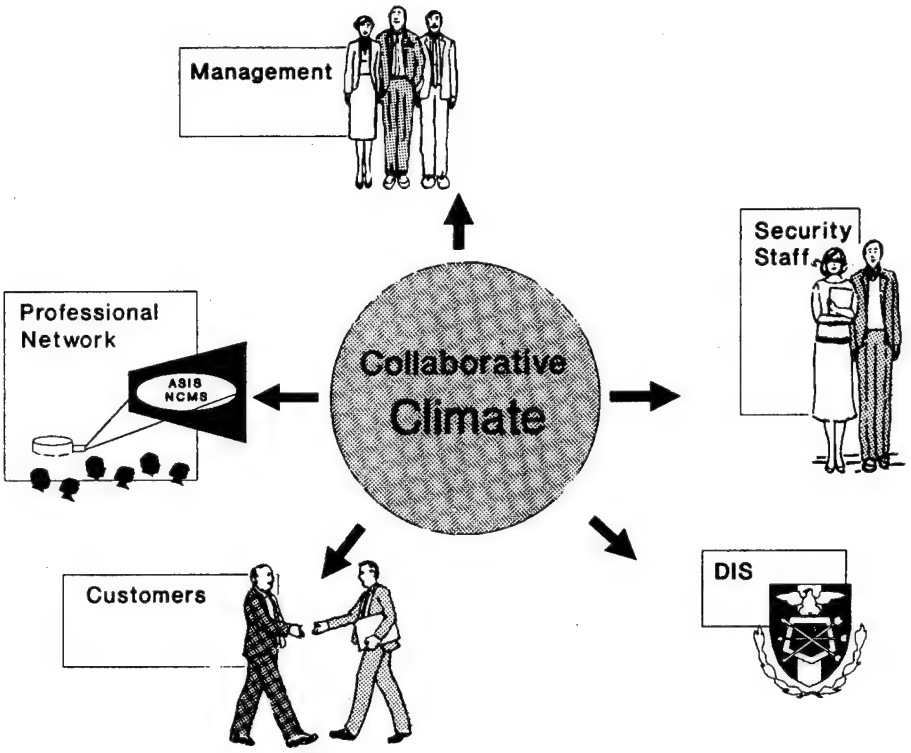
In *The Leadership Challenge: How to Get Extraordinary Things Done In Organizations*, Kouzes and Posner (1987, pp. 153-160) reported the results of a study involving 500 middle and senior level managers. In examining reports of the times the people in their study experienced a personal best in management, the authors found that fostering collaboration was critical for excellence. They cited six ways to build a system of collaboration and trust.

1. "Always say we."

Using *we* shares credit and establishes teamwork as the norm. FSOs tended to set cooperative goals for their department. They were also willing to share credit with their staff for accomplishments. This not only helped with security staff, but also affected dealings with others in the organization. An FSO from a rather large manufacturing company told us, "I try never to go to an engineer or project manager with *my* problems. Security is always *our* problem." He invoked the idea of a shared responsibility for security.

2. "Create interactions."

Creating physical and psychological opportunities for interaction was important. At a major computer firm in Silicon Valley, the scattering of small conference rooms throughout the workplace made it easy to gather key personnel for a few minutes away from the normal routine. Office design and layout, regularly scheduled meetings, designation of special teams to work on projects together, social gatherings, training seminars, and brown bag luncheons were some of the ways to get the job done better.



One FSO with a centrally located office made that office an informal stopping place for people crisscrossing the plant. With a sofa and a coffee pot, he created a hospitality suite. Not only was he able to keep himself alert to problems, he was also able to provide an environment receptive to ideas for improvement. Thus, he found an efficient way to increase the impact of a small security staff.

3. "Create a climate of trust."

Predictable leader behavior, honesty, reliability, preserving confidentiality and an open-minded approach to work were all examples of the qualities which define a trusting atmosphere. As one of our interviewees said, "The FSO who emphasizes trust and provides the example is far more likely to be told about security problems by his own staff rather than hearing about them from elsewhere."

4. "Focus on gains, not losses. Focus on opportunities, not problems, and create winners, not losers."

Having a win-win approach to conflict resolution and viewing problems as challenges were ways that FSOs helped create a climate of collaboration and trust in their organizations. Another simple way to emphasize the positive was to try to eliminate the use of the word but from one's vocabulary. In the words of Kouzes and Posner, "But stimulates disagreement at best, and more likely the beginning of an argument. But stimulates an either/or mentality and is antithetical to integrative and possibility thinking. Eliminating but from your vocabulary will free you from focusing on constraints and force you to consider the alternatives about how to make things happen. You may find it difficult to eliminate but from your vocabulary, but (well, we said it might be difficult) try, and see what happens" (p. 158).

5. "Involve people in planning and problem-solving."

Envision the FSOs at the center of a network of resources, the primary resource being the people with whom they must interact on a regular basis. FSOs act as a catalyst for the problem-solving process, bringing together the right people--those with the expertise to think about security issues. With clearly explained standards to be met, the people can achieve the greatest efficiency.

FSOs provided additional resources required by problem-solvers. These could take the form of connections, training, tools, money or even decision-making power. The function of the FSO was to keep communications open, monitor milestones, and periodically review progress.

6. "Be a risk taker when it comes to trusting others."

Demonstrating trust in others encourages them to trust you. Distrust always breeds distrust. Taking the first step in building trust in a relationship almost always involved risk. Being open and self-disclosing, as we have said before, was one way of demonstrating trust that invites reciprocation. Another was to create a reputation for dependability. Whether we are referring to an individual or an organization, dependability breeds trust. "Sowing seeds of trust with people creates the fields of collaboration necessary to get extraordinary things done in organizations" (Kouzes and Posner, p. 160).

By creating a collaborative climate, the FSO has laid the groundwork for establishing security support teams. These teams can provide the FSO with the resources, information, and backing necessary to achieve security excellence. Each support team will now be examined in more detail. Most of these teams are held together by informal networks and implicit agreements rather than a formalized structure. Also, the essence of a successful team is the giving and receiving of support in pursuit of shared goals.

THE MANAGEMENT TEAM

Perhaps the biggest challenge the FSO faces is to gain support from key managers in the organization. This support is essential in acquiring the resources necessary to successfully manage security programs. The task here is to be recognized as a team player. Before discussing strategies for being a management team player, we will briefly discuss what the FSOs meant by top management support.

Top management support. This support was the most critical factor in security effectiveness. Without top management support, even the best FSO in the business could not sustain an effective program. As one FSO stated, "I can't think of a single failed program where lack of management support was not a factor."

Support must be visible and active. It was not enough that the FSO knew support was there; everyone in the company must know. People need to see top management support manifested in policy and actions. Moreover, when asked to provide anecdotes of where they were getting the necessary support, almost all FSOs spoke of the CEO or president personally participating in security-related events. Support was not just words on paper; it meant personal commitment and physical involvement.

Top level managers other than the CEO or president were sometimes identified as the most critical in terms of supporting the program. This situation tended to occur in very large organizations where the division head, for instance, might be seen as the key leader and decision-maker, and the very top level of management hierarchy was located at a different site. Even so, the examples cited were similar. Only the titles were different. Active involvement and visible support were necessary at all levels of management.

Being a management team player. All the FSOs referred to themselves as part of the management team. They demonstrated that they were members of the team who could be depended upon in a crunch. Moreover, they saw their team as reaching into every corner of the organization. This required close coordination with every level in the organization. How was this done?

Not surprisingly, the FSOs used the strategies we discussed in the previous chapter. They gave many examples of techniques and behaviors related to being visible, credible, and professional. The feeling seemed to be: "If I want top management to consider me a part of the team, I have to prove myself." This is exemplified in the following illustration.

One FSO reported that when he had first started work he made a point of always showing up at the plant for every security glitch, even though the practice had always been to have duty security representatives assigned to respond during nights and weekends. He explained that he wanted to establish several points: he cared about the plant and its security, he was not above getting his hands dirty when necessary, he could handle a crisis, and as a manager he was going to be involved. Thus, he quickly established a reputation for dependability. He laid a firm foundation for achieving teamwork through his visible and active presence.

Another strategy for becoming a team player was participating in meetings. Although dismayed at the amount of time spent in meetings, FSOs attended when they saw an opportunity to communicate with the management team. Attending meetings also allowed them additional opportunities to exert influence on security issues. Almost all made a practice of having an open-door policy for other company employees. "An open door means access, and access means visibility. It also means more opportunities to sell security and to prove you really are a support operation," said one FSO.

While many of the FSOs became involved with the bidding process as soon as a classified RFP arrived, not all were as involved as they would like to be. Most simply reacted to the receipt of the DD254 or queries from others involved with the RFP review process. Some played a more active role by actually being designated as a formal member of the proposal team, taking part in the decision to respond to the RFP.

Whether or not this direct involvement occurred as a formally designated process, the message was clear. FSOs have to stay involved with the business side of the house, and supply expertise to top management. Being proactive about questioning customer security requirements is cost-effective. Every FSO could relate instances where their actions resulted in fewer dollars being expended for unnecessary security. TEMPEST requirements and Automated Information Systems (AIS) were areas particularly prone to overstated requirements.

Being persistent and having a plan for success were also important strategies for becoming a management team player. A new FSO wanted to become involved in the RFP bidding process, and security had never been included at his company. After a period of collecting information by SBWA, he decided that a lot of the resistance to security was the result of the image of being the cop who always said no. He researched past contracts and discovered instances where security could have saved money for the project managers. He informed the managers. He also made acquaintance (and ultimately established friendship) with the proposal manager.

Informally, he asked to review the next RFP and was able to point out security considerations that proved helpful to the proposal manager. Soon he was invited to attend the RFP meetings, and eventually became a fully participating member of the group. He understood the need to establish his own credibility before focusing on the change he really wanted. By his actions, he moved the security program beyond the mere compliance emphasized by his predecessor.

The analogy of eating an elephant, one bite at a time, was used to illustrate the value of persistence and patience for achieving management team support at all levels. The FSO described the effort it took, over an extended period of time, to gain the cooperation of one of his critical organization support peers, the facilities manager. Security had been viewed negatively in the company. The FSO recognized that support from the manager was vital to the future success of several initiatives being planned. The FSO's approach was to find out what the manager needed. From discussions with him and with others within the organization, the FSO determined that a chief complaint of the manager was that people always came to him wanting something--office space, furniture equipment, etc.--for which he had not budgeted or did not have the resources to provide.

The FSO offered to give something to the facilities manager, asking for nothing in return. He proposed that since security guards were on duty around the clock, making tours of the entire facility every 2 hours, they might be able to provide assistance to the facilities support function. He volunteered to have his guards report any problems in the physical plant concerned with lighting, plumbing, and the condition of entrances.

As he had hoped, the FSO received immediate and enthusiastic support from the facilities manager when the FSO eventually started planning for security improvements in the plant. He had shown that he was a contributing team player. He gave, and in return was given, support.

Communication was an essential part of being an effective management team member. One FSO in a high tech manufacturing company keeps all the top managers informed on security issues by sending a monthly report. This report details progress for ongoing security initiatives, potential problems, security issues occurring elsewhere in the industry, and any security information which may have implications for the company's financial management. He also attends the vice-presidents' meetings as the security advisor, where he participates as a team member.

Another FSO visited each of his principal company consumers (which might equate to department heads, project managers or product line vice presidents) to find out how he could support them. He tried to discover any special needs or concerns that security could help address. He sold security as a support program, better integrated his operation with that of the company, and created a lot of support in the process. Assessing the payoff, he said, "I don't see how I could have a better working relationship."

While security education and training programs are addressed in the next chapter, their role is discussed briefly here in the context of providing support to the management team. One program recognized the difficulty of having all managers attend pre-scheduled briefings. Top managers and project managers are supported in two ways. First, all senior managers are briefed individually. Secondly, each project manager and division vice-president is given a briefing based on the state of security in his or her program area.

Every problem area is covered, along with the appropriate security regulation or practice. Trends are discussed, as are DIS initiatives generated since the last briefing. The FSO stresses security performance as a service and support function. He makes the meeting an exchange of ideas and information about how the security function can be better accomplished.

One final method used by some FSOs to make security a part of the management team involves the handling of violations or inspection deficiencies. Here the project manager becomes part of the decision-making process. The FSO and the security coordinator meet with the project manager to discuss the violation's causes and possible solutions. Thus, the project manager becomes conscious of his or her role in security effectiveness and, having participated in solving a

problem, has a stake in the implementation of the solution.

THE SECURITY STAFF TEAM

When FSOs are a part of the management team, they provide support or service to other managers and in return receive support from management. Often the FSO does not act alone. In the larger defense contracting organizations, the FSO has a security staff that provides direct support in achieving security objectives.

Having a professional staff is one of the important aspects of gaining and keeping management confidence and support. The mix of tools may vary, but the message seems always to be the same: take care of your people, and they will take care of your business.

Developing the security staff. "You've got to be able to build a team, put it in place and let it run," said a senior security manager at a large high tech firm. Building a solid team starts at the initial hiring. The relative low pay in the security field was lamented, but most FSOs managed to persuade their own company to pay at above-average rates for security personnel.

FSOs told us that there is a rising customer demand for better security. The FSO must meet this demand by hiring the best people available, at a pay level designed to attract and keep them. One FSO in an eastern company told us, "I try to pay my people about 10 percent more than the going rate in the area. That way I feel sure I can draw the best and keep them. Our turnover is the lowest in the area."

In recruiting new staff members, FSOs prefer people who are already familiar with the company. They and their staff identify likely candidates. They use whatever media the company has available for advertising open positions. And they keep mental notes of what their staff tell them about interested coworkers.

When asked about qualities they would look for in selecting a replacement in the event of their own retirement or promotion, most FSOs agreed that security is a people-oriented business and those skills which focus on dealing with people are paramount. Management skill and experience was the number one criterion for new managers. As an FSO from a large multi-facility organization said, "I want management expertise! That's what this job is really all about. I can teach a good manager what he needs to know about security."

Another FSO said, "Managers need to be well-rounded and able to motivate people. They have to sell security with enthusiasm, but first they have to convince others right up to the top that they are worth listening to. Showing you've got what it takes to manage this complex monster is the way to do that." Others stressed ability as a team player, technical knowledge of business operations, and writing and speaking skills. A favorite quality was flexibility. One FSO summed up flexibility by saying, "This job is never the same from one day to the next. I love it! What was OK or worked yesterday doesn't work today. You've got to be ready to move in a different

direction on something, or use a different approach. If you can't adapt to the constant shifts and changes, you won't last."

Having found the right people for the security organization, how do FSOs get new people to a high level of productivity and keep them there? Giving high performers autonomy and opportunities for exercising initiative was a primary way of rewarding the best employees. "I can't lose. The best people thrive on being given greater responsibility and a harder job to do," one told us. He went on to say that the difficult thing was to know when he had given hard workers enough to test their capacity, and yet not so much as to lead to frustration and discontent.

Another FSO used goal-setting to enhance performance and motivate his subordinates. Although the primary focus was on security productivity, he insisted that each person establish at least one personal objective. "I like them to keep in mind that there is something in the process for them, as well as for the job." "It doesn't matter what it is, just so the focus is on them personally, not the job." One FSO emphasized the importance of providing individuals with feedback about their performance. "We're very open around here. I've told my gang I will always tell them immediately if I think their work is slipping. I expect them to let me know right now if they get overloaded. We work it out, and I always find a way to give them something they value in return for all their extra effort."

One example involving rewards was the use of time off. The FSO knew that an employee was a single parent and valued time off to spend with a young child. Time off was used as reward for extra performance. "It's like a family here. You know when they're hurting and what they need, and you give it when they deserve it. What you get in return is trust and a lot of hard work and long hours when things get tough, and no complaining." The ideas presented in Table 1 are examples being used to reward and recognize good staff performance. These are in addition to the normal company-wide incentive plans, merit pay systems and pay-for-performance plans.

Most of the FSOs stress participative management. They recognize that the security job is too big for one person to handle. They know that developing their staff to make the right decisions when called upon, and ensuring that they have opportunities to make those decisions, can mean the difference between success and failure in a security crisis situation.

Where FSOs had decision-making freedom and autonomy, they passed it along to qualified staff. FSOs usually talk over security issues with their staff, in groups or individually, before making decisions. When this is not possible, they try to review the circumstances with appropriate staff. Some FSOs establish task groups to consider an issue and make recommendations as necessary. Participants in such groups gain leadership and team skills, learn more about individual teammate capabilities, and broaden their understanding of the security program.

Job rotation was used to develop subordinates. This broadened the capabilities of staff members by shifting their responsibility to a different function within the security operation after they demonstrated successful performance in their current assignment. As one FSO put it, "Most of my people start with very little experience in either industrial security or government programs. I have to be able to show them, lead them through the steps, guide them to get the job done." One caution about job rotation: it may work best with employees who seek fulfillment in their work and who place a high value on jobs that require greater skill and effort. Finding employees with those motivations is the challenge.

Communicating with the security staff. FSOs hold frequent meetings with their staff, informing them of happenings that might have implications for security. An FSO told us that she started each day with a short staff meeting, usually standing around the desk or the coffee pot, where the events of the previous day were reviewed and the current day's agenda was set. In an informal setting with less structured discussion, important events often surface that may be passed over in a more formal meeting.

TABLE 1
REWARDING AND RECOGNIZING GOOD PERFORMANCE

** Use training as an incentive. Involve key staff in leadership/management training courses. Use DIS training quotas to reward best people who are eligible for the training. Take maximum advantage of in-house training courses. For multi-facility organizations, pull security staff together for periodic training and development activities. Invite top management to participate.*

** Encourage and assist high performers to develop presentations in specific areas, then give them company sponsorship to speak at professional meetings and at other company facilities.*

** Use small gifts (cups, key chains, tie tacks, lapel pins, etc.) as rewards for performance. Immediate and visible reinforcement can pay big dividends. Include all employees, not just security staff.*

** Use security team goal-setting with incentives.*

** Survey employees to find reward preferences. Have task teams develop incentive programs based on results.*

** Give special projects to staff who show initiative. Reward promptly and visibly for their effort. Examples given included setting up a security "Benny Suggs" program, doing a cost/benefit analysis for a proposed change, setting up and leading a task team, training a new employee, developing a new security education booklet, organizing a poster contest and managing a conference of security professionals.*

** Take the high performer to lunch. Arrange a staff luncheon to recognize significant achievement--either personal or professional. For example, a high school or college graduation, professional security certification attainment, promotion, completion of a major project (like installing a new classified inventory system) are all deserving of this form of celebration.*

** Publicize every award for performance through company media, security newsletters, personal memoranda from company executives, photos on company bulletin boards, etc. Personalize rewards as much as possible. Give a lot of personal feedback on performance. Deliver verbal "attaboys." Send memoranda of recognition of staff performance to upper management, with a copy to the individual concerned. Send letter acknowledging high performance to spouse, parents or both. Invite spouses to take part in recognition events.*

** Give cash awards.*

** Hold a security performance recognition event for those nonsecurity personnel (management and work force) who made significant contributions to the effectiveness of security programs.*

** Reward with opportunities to attend conferences or relevant courses. Sending employees to management seminars or a relevant course at a nearby college would benefit both the employee and the organization.*

One FSO said that he made a point of speaking with every staff member every day to share information that might be inappropriate for discussion in an open meeting. Another emphasized the importance of being attentive during meetings. One mistake many managers make is to consider staff meetings as a time only to have the undivided attention of their subordinates. They forget the importance of subordinates having the undivided attention of the boss. This FSO's emphasis was for everyone present "...to really hear and understand what is going on in the company, as it relates to security." He told us, "I found I can then often pick up signals that someone is bothered about something, or isn't totally on board with what is going on. By going to them afterward, I find out things I might never have known otherwise."

For multiple facility organizations, the FSOs placed great emphasis on frequent visits, not just for the periodic self-inspections but to show interest in the local security operation. In addition, the FSOs indicated the necessity of renewing contact with the line organization at remote sites both to emphasize the service orientation of security and to show that there were security resources available for special problems that might arise. Most FSOs in this kind of environment also took staff members along when visiting the outlying facilities. This encouraged communication and cooperation at the staff level.

Communication is important to keep security staff functioning as a productive team. Communication is also effective in informally increasing the size of the security staff by drawing nonsecurity personnel onto the security staff team. Several ideas were provided on how to accomplish this:

1. Form security staff hiring teams for new security personnel. They are informed of general requirements and are encouraged to develop them further by talking to the internal customers and other security sources. The teams recruit, screen, and recommend candidates to the Human Resources (HR) department or to a hiring committee. This may include interviewing prospective new employees. Security personnel must communicate security policies to the candidates and describe security needs to HR.

2. Hold "skip two" meetings once a quarter. These are useful in a large security department with several hundred people. The manager skips down two levels and meets with that level (e.g., the department manager would skip the salaried personnel and the supervisors and meet with the hourly personnel). The system works well for large organizations where frequent contact between the boss and lower-level employees is difficult. These meetings do have the potential to seriously alienate the middle managers unless they are kept informed or participate in the process.

It is vital that every employee has a periodic opportunity to have the ear of the top manager in security. As one explained, "You've got to get out and be with your people, on their turf if possible, to find out what's really on their mind and where communications might be breaking down." Some people require more structure to facilitate communication than others. Many will never volunteer the answer unless the question is asked. Therefore, ways to efficiently accomplish free and open exchange of information and ideas need to be found. This is particularly important in larger organizations.

3. Delegate primary management duties to an appropriate staff member when a major project is planned. Not only does this serve as a development opportunity, but the security project manager is forced to interact with others in the company to acquire and give information, sell security concepts, and represent the security department in a variety of ways. The more security staff are familiar with and involved in diverse parts of the security management function, the better able they will be to respond in an emergency, and the more effective they will become in handling their day-to-day responsibilities.

4. Choose an appropriate style for communicating with others. Some FSOs are comfortable with informal exchanges with their staff. Others prefer a set schedule and formal agenda. The point is that all had made some assessment of their environment, personal preferences, and the responsiveness of their staff, and had developed a style that worked for them. Virtually all the FSOs we interviewed told us that they had given much thought to improving communications. It seems that most of their approaches to communicating had evolved from their skills in dealing with a wide range of personnel during their careers.

5. Be attentive to productive security behavior of company personnel and reward it publicly. As previously mentioned, such rewards take almost every form imaginable, from tie tacks with security logos, coffee cups, memo pads, pens, large plastic security paper clips, to decals. Special security "attaboy" posters, formal company letters, hosted luncheons and articles in company newspapers were additional ways these FSOs used to ensure that those who practiced good security were recognized and publicly rewarded.

6. Carry a collection of security "doodads" during SBWA forays and give them away to company employees. "They always get my smile, good words and a handshake. This is a tangible reminder that observing good security is valued in this company," one FSO explained. Such practices were seen not only in terms of rewarding past behavior but also of being a positive reinforcement for good security behavior in the future.

7. Take immediate staff to lunch periodically. One FSO also included someone who had been especially security-conscious, had made a valued security suggestion, or who was cited by the DIS inspectors for cooperation and good performance. This served as a visible signal of approval. Another approach for rewarding those cited positively during inspections was asking the DIS Industrial Security Representative to specifically mention these personnel to the senior manager during his final briefing of inspection results. He would then follow up with a formal letter of appreciation to the employee, signed by the FSO or someone at the highest level possible. In one case, copies of the letters were posted on the employee bulletin boards scattered throughout the organization.

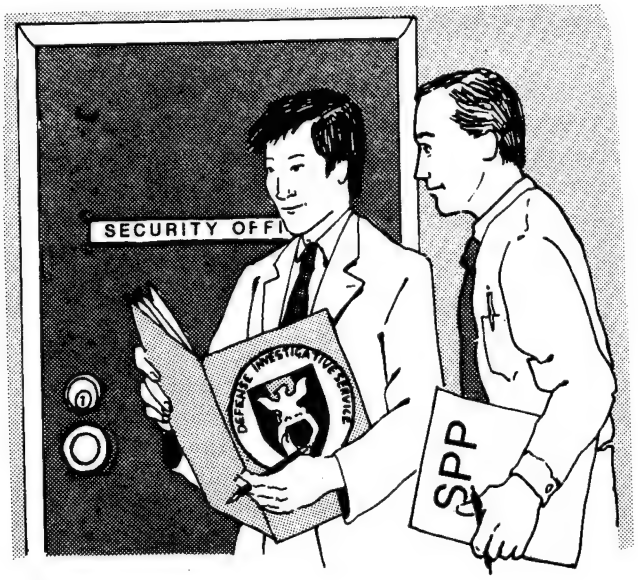
THE DIS TEAM

In addition to building and maintaining a cohesive security staff team, the FSO has a key relationship with the DIS inspectors. When asked how they ensured the most effective and problem-free relationship with DIS, the FSOs most often said something like, "...by being as honest and candid with them as possible, by never playing games with them, and by treating them with professional respect." An FSO with extensive experience both in and out of government told us, "I treat them as one of my most important resources, and they know it." Another spoke of DIS as a valued customer, and said that he always tried to think of the relationship in those terms, especially when there was conflict. In essence, most FSOs viewed DIS inspectors and themselves as being on the same team, with a common goal of protecting classified information.

In all but a very few cases, DIS was cited as the first place FSOs would go when faced with security issues they could not resolve from their own experience. While acknowledging that the relationship was not always smooth and that there were things that could be done by both sides to improve it, most FSOs had experienced positive change in their relationship with DIS during their tenure. "What we get by being honest with DIS, by being candid about our state of security, is trust," explained one FSO.

Open communication seemed to be the key characteristic of the DIS relationship. It creates an environment where the partnership can thrive: "I know I can call my IS representative about a problem, and he won't overreact and make the problem a crisis. Why? Because we talk, and we talk a lot. He knows me and I know him, and we

trust each other." This FSO went on to tell us that it was important not to overload the representative with calls, but not to hesitate when it was necessary. "After all," he said, "it is his job to support us, just as it's my job to support the DISP."



We call this collaborative approach Partnership Plus. First, the FSOs supported the DISP through compliance. Next, they went beyond compliance by volunteering to host DIS training sessions and provide facilities and support for DIS conferences with contractor security managers. Many had agreed to serve on industry advisory panels for security issues and to participate in Department of Defense Security Institute (DSI) training conducted for both industry and government personnel. Several had written articles for professional publications and in other ways had taken the initiative in calling attention to or resolving government security problems.

In short, FSOs do not wait for problems to come to them; they identify problems and take action to resolve them. The FSOs would prefer more communications with DIS. Some were even concerned at the possibility of receiving less frequent inspections. "DIS gives us a good look and they help me keep the security emphasis visible in the corporation."

Such visibility was seen as an important product of the relationship. Many FSOs made a point of introducing the DIS representatives to their staff, security coordinators, project managers and top management whenever the representatives visited, and always when new DIS personnel were assigned. FSOs were also strong advocates of the DIS resident representative program. The permanent presence of DIS in contractor facilities was viewed as mutually beneficial. Most FSOs were in favor of the DIS/industry partnership concept, and most expressed a willingness to do the things that may be necessary to make it work.

The following three strategies were used by FSOs in their relationship with DIS:

1. Practice openness and honesty in dealing with your DIS representative. The result of reciprocity is trust, and that is what makes the partnership work.

2. Emphasize both quantity and quality in communications with DIS. The more communication that takes place, the better the relationship. At the same time, the content of that communication must be substantive, and enhance the image of the FSO as a professional who contributes to the partnership.

3. Be willing to go the extra mile in supporting the partnership concept. Bring solutions to the table when there are problems, and take the initiative to implement solutions whenever possible.

THE CUSTOMER TEAM

"This business wouldn't be nearly so difficult if it weren't for the customers," mused one of our interviewees. "Of course," he went on, "it wouldn't be as exciting and challenging either--and we wouldn't be having this talk, would we?" In those words he summed up the goal of government security managers everywhere to

provide support to customers whose exacting demands seem to call for only one standard: zero defects.

Meeting this goal is complicated for many defense contractors when they also serve a variety of government customers for a wide range of programs requiring different degrees of special access. Almost all FSOs had several such programs to manage, in addition to their normal DISP responsibilities. Lack of common security standards, frequent changes in interpretation of requirements, and changes in customer program managers are a few of the problems. How did these FSOs manage these challenges? They worked collaboratively with the customer's security representative to meet security requirements.

It is not surprising that the same techniques that work in the internal environment also work in creating effective working relationships between FSOs and outside customers. Openness and honesty in communications, frequent and substantive interaction, and a Partnership Plus approach make it work. The FSO becomes the driving force giving the customer a sense of satisfaction.

The FSO of a large electronic components manufacturer said, "We have a reputation for consistently high security marks. We got that by applying the highest standards possible to every contract, by making sure that everyone involved knew and adhered to those (standards), and by doing whatever it takes to satisfy the customer." This last point is important. Doing what it takes does not always mean doing exactly what the customer initially demands.

FSOs reviewed security requirements carefully, looking for more cost-effective ways of meeting the requirements, and trying to identify those that might be unnecessary or overstated. They also looked for the missing elements--those that might be required but which were not stated and which might need additional planning and resources. As one FSO said, "I owe it to the company to provide cost-effective security for our customers. I owe the customer the highest level of security protection required by the contract. Finding ways to make those two things compatible is my first challenge, and convincing the customer that they are compatible is my second."

One FSO met these two challenges by reviewing unusual requirements personally with the government security monitor officer. This was important for several reasons. The first is that this process may lead the contracting officer to revise the requirement without confrontation. The FSO focuses on gaining clarification on the requirements and their rationale. This low threat approach often leads to self-initiated change. The second is that the review may reveal elements of the contract not made clear in the RFP or the DD249. The third reason, and perhaps the most significant for the customer relationship, is the signal that such an approach sends. How better to demonstrate a desire to understand and respond to the needs of the customer than by working collaboratively?

Another method for fostering teamwork with the customer is by literally getting closer to the customer. Ensuring that security is a part of the meetings that take place between customer representatives and company personnel during customer visits is a common practice. On-the-spot response to customers' security concerns, raising questions about security requirements (especially when there are contemplated changes in contract specifications), and serving as security advisor to the project manager are all useful practices.

THE PROFESSIONAL NETWORK

We need to comment on one final strategy: FSOs' use of professional networks. We already discussed how much FSOs rely on extensive communications in every phase of their work. The same level of communication is required with their professional relationships outside their organizations.

There are many professional security associations. Effective FSOs are the lifeblood of such groups, which, in turn, sustain them in their desire to learn more, share their knowledge, and develop their profession. Most belong to more than one professional security management association. Most are also members of the American Society for Industrial Security (ASIS) and the National Classification Management Society (NCMS). A majority have been officers in those groups. These individuals are actively involved, often contributing more than their share of time and talent towards accomplishing association objectives.

There are other local and regional resource groups that serve the same purpose. Such groups are generally special-purpose, meeting a more narrowly defined need. One example is the local area groups that have been formed to share security education ideas and resources. Several of our interviewees were instrumental in establishing such groups in their areas and providing assistance and support for others who want to develop similar groups.

Another resource used by these FSOs is the DSI headquartered in Richmond, Virginia. Not only have most FSOs been recipients of DSI training, they actively encourage their staffs to participate whenever possible. More than a few use the incentive of DSI training to encourage improved staff performance or as rewards for outstanding achievement. Several have also served as resources for DSI training, making presentations to student groups, participating in panel discussions, writing articles for DSI publications, and providing input to course revisions.

Some FSOs teach college courses. They are involved in several different curricula areas, chiefly those relating to security or general management. One FSO who taught courses said, "I certainly knew the capabilities and potential of my students. So, when a staff position came up, I knew where to look." Other FSOs served as guest lecturers, made presentations to local civic organizations (many also belonged to the organizations), or wrote articles for the several professional security organization publications. FSOs are active proponents of the security management profession. They establish high standards and support its developmental training.

SUMMARY

The second component of security excellence is building support teams. As discussed earlier, the redefined FSO role provides the first step for moving beyond compliance. This expanded role then serves as the groundwork for establishing a collaborative climate which in turn sets the stage for building security support teams. The final step of the security excellence challenge involves the development and implementation of security education and training programs.

CHAPTER IV

DEVELOPING SECURITY EDUCATION AND TRAINING PROGRAMS

> "The more you can make security a personal issue...actively involve them...the better your program will be."

Our first impression of the security climate in an organization was usually obtained by walking into the lobby area. We observed how we were received by security personnel responsible for processing visitors and noted the visible reminders of security--posters, placards, visitor logs, badges and surveillance cameras. We also noticed the way other company personnel interacted with security guards and staff. All gave hints about the security education and training program at the organization.

In the previous two chapters, the importance of redefining the FSO role and building security support teams was emphasized; these steps provide the groundwork for developing effective security education programs. From another perspective, these same steps enhance security awareness and motivate employees to follow security requirements. In discussing security education programs in detail in this chapter, many of the strategies introduced earlier are revisited.

During the research, we saw many security education and training programs that differed only in specifics. The FSOs all took the same basic approach to getting the most out of their education and training effort. They used similar terms in describing the characteristics of a successful security education program. Some may have had more resources or been more creative in implementing program elements, but they all seemed to use the same model.

There are three basic areas into which the components of security education programs fall. The first area, determining the requirements, involves assessing training requirements and developing a plan. The concern here is with defining what employees need to know and developing a way to communicate the information. The second area, getting resources, involves acquiring the materials and personnel necessary to conduct the training. The final area, motivating security performance, is the key element in moving beyond compliance. It involves ensuring that employees not only learn their security requirements but are committed to performing them.

DETERMINING THE REQUIREMENTS

Needs assessment. FSOs tapped every possible resource to discover security education and training needs. "You can't just do what the ISM says and be satisfied. The (ISM) manual sets the minimum standards. We know that's not always enough to ensure the level of security we feel comfortable with." The FSOs always went further than mere compliance in providing education and training.

Many companies include all employees in the initial security orientation briefing. Others have designed special security briefings for noncleared personnel. As one FSO said, "Even the employee who has no clearance and who will not be working in a cleared area should have some understanding of the security climate that exists here in the company. Employees need to know what to do in the event they are inadvertently exposed to classified material and the reasons for security procedures." The FSOs decided that they needed to go beyond the basic requirement to hold security briefings for cleared personnel.

Although there were only a few who conducted a formal needs assessment, all FSOs had some way of monitoring changing needs. Many reported that SBWA helped to identify unmet security education needs. "When I am out and about in the plant, it doesn't take me long to see where the gaps in our training are," said one FSO in a manufacturing facility. "Not only can I see what they are doing and how they are handling their classified documents, but inevitably they also ask me questions or have casual conversations which tell me a lot."

There were a number of other ways in which the FSOs improved their assessment of security education and training needs. Here are a few.

1. Periodic security knowledge surveys are distributed either by interoffice mail systems or in security newsletters. These surveys may be used to check knowledge of handling and marking procedures, physical security safeguards, visitor or visit request procedures, and other general security requirements. The same process may be employed to check continuing familiarity with special program requirements.

2. Security hotlines exist for receiving questions or comments from security-conscious employees. "We got a lot of calls from one group about classification, so we decided to set up a special training session just for those employees," said one FSO.

3. Security improvement suggestion forms are prominently displayed in all areas where cleared personnel work. Some type of award, from certificates to cash, is given for every suggestion adopted. Usually there is also some level of recognition simply for making the suggestion--a letter or memo from the FSO, for instance. It was often reported that the number of suggestions, many quite good, increased after every public recognition of a winning suggestion.

4. Security brown-bag lunch meetings are held regularly where anyone can discuss security issues. A variation is to designate a table in the cafeteria for such informal meetings.

5. A free coffee day is organized in the security office to encourage employees to drop in and discuss security questions.

6. Self-inspections are conducted by the security staff who are tasked to look for training and education deficiencies. The self-inspection program gives the security staff an opportunity to conduct very specific education and training in the areas most likely to receive DIS attention.

7. Periodic meetings are held with line personnel working on new classified contracts. The purpose of these meetings is to identify potential security problems that might not have been covered previously.

The challenge of making sure that all education requirements were met invariably came up in the interviews. For example, many of the companies had contracts with several agencies. They often included classified contracts with customers who were not subscribers to the DISP. In these cases security requirements often differed in substance or interpretation, complicating the task of providing education and training. The solution was to define the requirements of each customer.

This was accomplished by ensuring complete understanding of the contract and the various security implications. This usually meant a

thorough review of the DD254 with the customer or security representative. The intent was to be clear on security interpretations and on any areas where special education and training needs might exist.

Once the customer requirements were reviewed, the focus turned to the division where the work was to be done. FSOs identified the personnel assigned to the project, the security training already completed, the skills and experience of the security personnel, the special requirements which might alter the security environment, and the need for new or additional personnel to be assigned. Most tried to involve the project manager or director in this process as much as possible.

The final step was to meet with the security representative and the principal managers who would be responsible for the contract and security procedures. This step included explaining the results of the review, setting education and training objectives, and developing a plan for accomplishing the objectives.

Most FSOs followed the above process. The details and formality varied, of course, depending on the size of the organization, the nature and size of the project, and the individuals involved. Some developed and published formal plans for internal distribution. Other FSOs were less formal and handled coordination by memo or personal contact. They had all thought about what was needed and how they were going to accomplish it. They then had a plan and could readily refer to it.

Considering the large number of contracts and security education activities required to support the DISP, it is easy to see why completing this process is difficult at times. It also becomes clear why nearly everyone in the security departments had education and training responsibilities, regardless of their primary assignment.

Program plan. Most FSOs had a plan for implementing their education and training

program. A few of these plans were detailed, with flow charts, lesson guides, and weekly or monthly schedules. Others were less detailed. The level of detail depended on the type of facility, number of employees, and the scope of classified work being done. Even though most had a plan of action for accomplishing training and briefings, many also discussed the need to be flexible enough to accommodate any unforeseen requirements.

Most of the FSOs felt that formally scheduled activities represented only a minor portion of the total security education and training. "I will be very honest with you," one FSO said. "Most of our best, most productive security awareness briefings are done by me and my staff, one on one with the engineers and others out in the facility. We'll get a question or see what they are doing, and that opens the door."

Nonetheless, the planning was useful for ensuring that time was allocated efficiently and minimum training requirements were met. Some plans were distributed beyond the security

department, some were kept and monitored using a personal computer, others were kept in notebooks by the FSO or education and training staff. In one instance, a plan was simply noted on the FSO's quarterly and monthly calendar. The form of the plan was not important. But the planning process was important; the FSOs knew the training needs and requirements, and had a plan for meeting them.

Timing. FSOs pay considerable attention to timing when implementing education and training plans. For example, the introduction of a new automated information system calls for carefully phased training as the implementation proceeds. There are optimum times for security aspects to be covered. Timing considerations are a part of the normal planning process.

Being involved early in the RFP process, for example, was particularly beneficial. "If I can get in at the beginning of the bidding process, I can start planning what we will have to do and when." If they are not included early, FSOs are forced into a reactive stance. Many FSOs reported being proactive by examining the subject areas, identifying potential training needs, and developing ideas for addressing them. Some of the areas are developed further, while others are saved for possible use in the future.

Thus, FSOs are ready to respond to opportunities that arise in the future. As we were told, "It doesn't do us much good to hold a training session on visitor control for a project that has just been put on hold. We've got to be flexible enough to ignore the plan, if necessary, and either cancel or substitute with something more appropriate."

The following quote underscores the importance of anticipating training needs. "After our DIS inspection, we always have open slots for security training. We introduce subjects where we might have been deficient or which may need additional effort. You might say we plan for the unplanned." Another important aspect of timing is the ability to sense when the time is right and then being prepared to respond. The FSOs are confronted by training opportunities every time they practice SBWA. They enjoy these brief training encounters and the chance to influence security behavior by giving advice.

One FSO reported an instance where timing and a readiness to take advantage of opportunity paid off. Previous requests to initiate a system for bar-coding classified documents had gone nowhere due to concerns of higher management related to the expected return on the investment. The required hardware and training were not cheap. After suffering from deficiencies cited during a customer's inspection, the proposal was updated, re-submitted, and approved.

GETTING RESOURCES

Staff expertise and access to resources. These two elements enabled the FSO to carry out the responsibilities associated with security education and training. In large and small companies alike, there was great emphasis on using every possible resource to accomplish education objectives. Where staff expertise existed, a considerable amount of the training was delegated. Even so, we found that most FSOs liked to conduct at least part of the training and briefings. Where staff expertise did not exist, the FSOs developed it. One area where this often occurred was in Automated Information Security (AIS).

One FSO in a small electronics firm was a one-person operation with little computer experience. Seeing the need for more AIS security expertise, he canvassed the company and found an individual with the appropriate background. Going to this expert with questions resulted in increasing the FSO's knowledge and also increased the expert's level of interest in the area. Gradually, the FSO taught the expert more and more about security programs. The expert gradually became a de facto member of the security team. The computer expert now handles all the AIS security projects as well as the training and briefing responsibilities.

In another facility where an FSO held periodic training for his staff, outside experts were often used. "They get the message from me all the time. I keep it fresh by having people from outside the company deliver it," he said. He brought in FSOs or security staff with particular expertise from other companies. FBI counter-espionage specialists, CIA and DIS personnel, and local university faculty were excellent teachers of security. "When the professional spy catchers talk about the threat, people listen." These outside professionals also generate interest beyond the immediate security staff. This FSO said he now had many requests from nonsecurity personnel, including senior managers, to attend his training sessions.

There were some novel approaches to using personnel within the company. Inviting company engineers to talk about new technology and the security challenges raised by the technology--particularly in telecommunications--was one approach. Putting together a panel of nonsecurity employees to discuss their views of security issues in specific programs was another.

Yet another approach was the creation of a consortium of companies to share resources and ideas. The company representatives met periodically to discuss ideas, share lesson plans and posters, and develop collaborative projects. One project was the production of a video security briefing which could be tailored for each company by changing the logo, organization charts, etc. Together, the representatives had the necessary technical capability, funding and personnel expertise. Other such ideas included special program briefings, company-specific videos on classification marking, handling and accountability, AIS requirements, and taping of special presentations which might be shared with others in the group.

Lack of resources was a challenge to initiative and creativity. The FSOs made an effort to develop their staff's skills in areas of need. In addition, they developed networks of experts who became routine sources rather than being sought out only in a crisis. Finally, FSOs involved themselves in every aspect of the security education effort, from planning to execution.

DoD resources. DIS places great emphasis on education and training. Industrial Security Representatives in every region of the country agreed with the FSOs that education is necessary for a successful security program. Moreover, DIS stresses the importance of assessing these programs during their periodic inspections. As one Director told us, "The main thing we get from the private interview part of the new inspection procedure is how well a company's awareness training is working." DIS regions have established positions for education and training specialists whose primary duty is to support the contractor organizations in improving programs. DIS also encourages contractors to establish training and education support groups.

DSI is also an important contributor to security training within the DISP. It conducts training for contractor facility security officers as well as for the DIS industrial security specialists. A large portion of that training covers responsibilities for security education for contractor employees. They make training more readily available by the use of mobile training teams. In short, there is continuing emphasis on security education and training by both DIS and DSI. FSOs build on this and make use of government resources.

MOTIVATING SECURITY PERFORMANCE

Employees are motivated to be security-conscious in many ways. They are more motivated when they perceive that top management and supervisors care about, support, and reward meeting security objectives and participate in helping define security procedures. Their motivation also is increased when the security message is stimulating and makes sense in the context of their specific jobs.

Management involvement. We kept coming back to management involvement and support as

the key ingredient for success, no matter what the topic. "If top management isn't behind your program, you can bet you'll have a hard time making it work." The key index most FSOs used to gauge the level of support was the degree of actual involvement in security education activities by those at the top of the organization: do the executives participate in security activities and briefings?

In many companies, executives actually gave portions of the security briefings for new employees. In one company the contract project manager, together with his superior, the product line manager, were given project security briefings by the FSO. CEOs wrote articles for the security newsletter about the importance of effective security. Top managers took a leadership role in officially recognizing outstanding security-related performance. The CEOs sometimes even wrote personalized letters to individuals cited for exceptional security performance. They knew the potential impact of a security failure and did not hesitate to get involved in efforts designed to ensure security success.

Top management support and involvement was considered effective only if it was consistent. Such participation and support had to be seen as routine and expected, a part of the company culture. How did it get that way? A great deal of credit must go to the FSOs. They were persistent, innovative and persuasive in getting top management involved. "We haven't had anyone from the executive suite enter our poster contest yet, but I'm working on it," one FSO told us.

In Chapter II, the leadership characteristics of the effective FSO were discussed. Certain of these characteristics deserve reemphasis, particularly as they apply to the involvement of management in education and training programs. As one FSO said, "First and foremost, I've got to sell security to the president and the vice-presidents. In addition, I've got to have all the skills of the supersalesman to do it well." This seemed to be the case particularly when talking about education and training programs.

Pointing out the healthy financial results of an effective education program was a good way to influence upper management. Many FSOs talked of other companies whose security programs had failed. They knew the amount of company work done under classified contracts, and the dire financial consequences of withdrawal of certification. Stories were told of contracts won at least partly because of past security performance, or lost because of nonperformance.

Methods for getting across to top management the message of effective education varied widely. "We have established a reputation of getting the job done by high impact and low cost solutions," one FSO explained. "So when we ask for something extra, we get a sympathetic ear." Another expressed the same idea. "It's part of the credibility thing. When I ask for something that costs more than usual, I can always show how it will make us better or that it will be cost-effective in the long run. I've never failed to get the support I really need." There was a mutual trust between top management and the FSO and an underlying focus on financial results. Few problems existed in getting senior management support, and with this support, the stage was set for excellence.

Employee involvement. The second factor contributing to successful education and training programs was employee involvement. "The more you can make security a personal issue, identify and speak to individual concerns and actively involve them in the practice of security," one FSO told us, "the better your program will be." The large group employee briefings were necessary to meet DIS requirements, but small group or one-on-one, limited-scope briefings were far more productive. Discussion groups, active security suggestion programs, rewards for exemplary performance, and participation of top management in security-related activities were ways to encourage employee involvement.

One FSO established a program, built on employee participation, to improve parking lot security for employees. The problem had become

acute because of auto break-ins, pilfering and fear of assaults. The program was immediately successful, catching an auto burglar in the first week of operation. The employee who reported the incident was given a financial reward, and the event was highly publicized. The result was an increased awareness by employees of the services provided by the security department and a greater appreciation of the scope of their own responsibilities. Security's image as government watchdogs and the guys who always say no had changed. There was an immediate increase in drop-ins and telephone calls asking about security procedures and suggesting changes to improve security. The security department, through employee participation, generated interest in other aspects of security.

Another example of employee involvement occurred in a Silicon Valley electronics company. As a result of an employee suggestion, the security department instituted a program to fingerprint the children of employees. The fingerprint cards were then given to the parents for use in the unlikely event that their child were ever missing.

This effort, conducted with the cooperation of local police, showed that the security department was a true service organization with a broader interest in the employee than mere compliance with regulations. This company saw its education and training responsibilities in a larger framework than just the ISM or the DISP--and the payoff was greater employee identification with the security department and, ultimately, better support for its objectives.

Consumer focus. FSOs and their staffs reported that a successful education and training program could only exist where there was strong consumer focus. One FSO described the company's employees as constituents, a term that underscores a customer orientation. She went on to explain, "I view it as a two-way relationship. The employees are at the same time supportive of and supported by the security department. We need to give them the best possible support in their efforts to maintain a secure work environment." Support meant the knowledge, training and structure required by every employee to respond to security needs. Included was the ongoing assistance provided by the security department, comprised of refresher training, administrative support, and monitoring functions.

There are many different consumer groups for security education in the typical company. One list offered by the training and education specialist at a major shipbuilding firm illustrates the number and diversity of possible consumer groups. His comprehensive Audience Targeting List includes:

* Senior Management
* Supervision
* Security Representatives (Coordinators)
* Cleared Employees
* Derivative Classifiers
* Custodians of Controlled Areas
* AIS Personnel/Operator
* New Hires
* Overseas Travelers
* Lunchtime Security Monitors
* Contract Administrators
* Offsite Activities
* Subcontractors
* Vendors and Visitors
* Special Access Program Employees

While the list certainly will not be the same for every facility, it does help emphasize two points. First, there is a need to identify the consumers of security education. Second, the needs of these groups should be considered in selecting the content of the training and the media to deliver the message.

However, tailoring security education materials can go even further. There is much to be gained by bringing the security briefing to the individual level, directing the briefing to particular jobs. "People really listen when you can put the message in terms that relate to their specific job, rather than just generic security requirements." The best way to ensure success is to know as

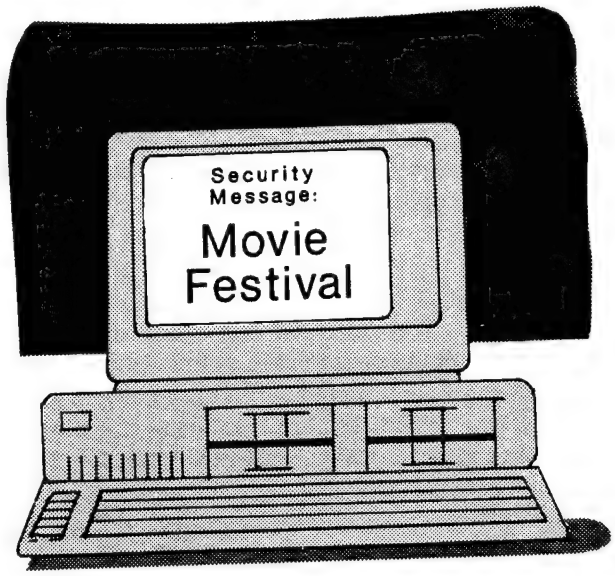
much as possible about the consumers in the context of their job.

Message delivery. Many employees are bored by traditional classroom teaching methods and lectures. Professional trainers know this and encourage learning through exercises and discussions. Such training usually includes actually either doing the task or a simulation. Much of the training was of this type. Classification and marking rules were taught not only by telling the employees what the rules were, but also by showing them examples, going through the process with sample materials, and providing individual follow-up by going to the employee's work area and reviewing specific work-related documents.

Visual training aids were liberally used. One FSO said, "We are a TV generation. I have found that video is very well received and tends to generate a lot of follow-up discussion, especially if it is done professionally." We saw several examples of locally produced video materials that were of excellent quality. Even though a company may not have the facilities to produce such media, collaborating with other companies can reduce the cost for all. In addition, there already exist extensive video resources, both in industry and commercially. The FSOs knew where and how to acquire them and did so regularly.

Liberal use of handouts was also effective. "Never let them walk away from a training session without something in their hand," was a common comment. Printed material seemed to be the most used visual aid. As evidence of the industry practice of sharing, we also saw many materials that were adapted from different companies. As one FSO said, "We try to help others to keep them from reinventing the wheel." He assured us that any assistance given was usually returned many times over.

The recently completed *DD254 Handbook*, published by the National Classification Management Society (1989), is an outstanding example of a collaborative industry effort to create needed security resources for widespread distribution. It is a step-by-step guide that leads the reader through the DD254 form in great detail, explaining options and interpreting the content of specific entries. It will probably become a standard training text for the industry and is an excellent reference volume.



The idea of using both industry and commercially produced videotapes for a company security movie festival has caught on. Such a festival is generally held over a week-long period, and offers free popcorn and other refreshments. Attendance during the noon hour has been excellent and the feedback favorable. Interviews with Soviet defectors and convicted spies, briefings by security experts, and security educational topics make up the bulk of the available videotapes. Another option is to show the videos during the night shift or immediately before a work shift begins. We also heard of video projects that take the viewer through typical company work spaces, showing obvious and not-so-obvious security weak points, and explaining company procedures for ensuring security. These movies use actual

employees and company security staff as actors, which adds to their appeal.

Sometimes the simplest ideas pay off. One FSO described the problem of getting people to pay attention to security newsletters that were distributed to employees. The solution was to print the newsletter on a color of paper unique to the security department. Anyone would be able to identify it quickly. Finding a special color in a large organization might be difficult, but the enterprising FSO will probably come up with a special logo or some other distinguishing feature.

We heard of a number of good ideas for making printed materials more understandable. Here are a few.

1. Using a specially designed desk guide for security reminders (e.g., telephone security, scheduled DIS inspections, classified storage rules and procedures, AIS, and the instructions for reproduction of classified material).

2. Publishing an appointment calendar with security messages, quotes and security-related artwork or cartoons for each month. One calendar has each month represented by reproductions of the best selections from past company security poster contests. Special security events are highlighted each month, as are other important dates, such as paid holidays, recreation events and stockholders' meetings.

3. Affixing a "Think Security" plastic paper clip to all security-related printed communications. Others used colorful stickers to achieve the same purpose.

4. Inserting security messages into the log-on sequence for all classified computer systems.

5. Using a distinctively designed cover sheet for security education and training-related material.

6. Including security-relevant word games, crossword puzzles, acrostics and cryptograms in security newsletters and company newspapers.

7. Occasionally inserting an employee's name into the text of one of the newsletter articles, with instructions to call security by a certain time. When the individual responds, he or she receives free lunch or movie tickets.

8. Entering the security procedures manuals into the internal electronic mail system, facilitating access when questions arise.

Effective education and training activities grab attention, hold it while the security message is being sent, and lock it into the mind of the audience. A boring presentation, whether it be a briefing or a printed page, sends a message that the subject may not be especially important or worthy of attention. Creative use of media not only stimulates the target audience, but can also make an otherwise routine subject interesting. Everyone knows, we were told, when a briefing is being given just to "check the box."

Stressing an individual's security responsibilities during training is very important. For example, one FSO told us: "Every employee must feel responsible for security. Security comes from within the employee." Success can best be measured by how well the cleared employee becomes motivated to join the security team. The following statement seemed to sum up the notion: "I try to make every cleared employee a security manager--someone who is not just aware of requirements and procedures, but someone who is conscientious and consistently reliable in meeting security responsibilities."

We have already talked about some of the efforts of FSOs to get the security message to the individual employee. But, getting the message there is only the first step. The most important thing is to have the employees internalize security. Accomplishing this is an enormous challenge. As one FSO explained, "I know it's too much to expect that security is number one with people; the job itself is usually number one. What we try to do is increase the chance that security is at least number two."

Attempts to increase an employee's security consciousness are more likely to succeed when the education and training are oriented to the individual. There were many examples of individually oriented education. One was the practice of having the employee assist the security personnel in making a periodic inventory of classified holdings. Another was holding sample, private interviews with cleared employees during semi-annual security audits, like those conducted by DIS as part of their new inspection procedures. In one company, cleared employees from other departments were routinely invited to attend security staff training when the topic was of interest. They were encouraged to participate fully and, in effect, give a shop-floor perspective. In several facilities, periodic security reviews were conducted for specific project areas, using nonsecurity personnel to bring up problems for discussion and resolution.

Another approach involved setting up a problem-solving team for security. This volunteer group would consider specific security management issues. Examples included questions like, "How can we conduct necessary security audits and reviews that involve the employee, yet minimize the negative impact on productivity?" Security staff usually chaired such groups, but the groups mainly consisted of nonsecurity employees.

One FSO played a major role in indoctrinating all new employees. Each individual was personally interviewed by the FSO in the security office and briefed on the security responsibilities of the company to its customers. The individual's own responsibilities were also explained. The safeguarding of proprietary information was emphasized, and the rules covering normal government classified work were described.

The new employee was then taken by the FSO on a guided tour of the facility, during which security procedures were explained. The tour ended in the work area where the employee was assigned. There, he or she was introduced to the security coordinator and briefed on specific security procedures which the employee would encounter. Part of that briefing was given by the supervisor. This showed how security was the job of everyone in the leadership chain, and that the individual was the cornerstone of a successful security program.

Enthusiasm. Finally, we present the element which makes everything else work. Without FSO enthusiasm any program will eventually founder. A sure way to stimulate discussion in the interviews was to ask about security education and training. There was no doubt that effective FSOs were very involved in training.

When we asked, "Who is your head trainer?" the predominant response was simply, "I am!" When we indicated an interest in acquiring a representative sample of the brochures, posters, program outlines and publications the FSOs were particularly proud of, we became inundated with samples. Some of these materials we had already seen at other companies. One FSO responded, "We share freely when we come up with something good. That helps us all, particularly those who don't have large staffs. The bottom line is that we are all in the business of serving national security as well as our own security interests."

SUMMARY

This chapter has described how FSOs develop and implement their security education and training programs. They determine training requirements through needs assessment and develop plans for implementing these programs. They are creative in getting the resources necessary to get the job done. Finally, they combine management and employee involvement with their own enthusiastic leadership to ensure employee commitment to effective security practices.

Chapter V

CONCLUSION

The future just ain't what it used to be.

-Yogi Berra

This report has presented an overall framework for viewing security excellence and has demonstrated that moving beyond compliance results in more effective and efficient security programs. Eleven strategies are used by effective FSOs to redefine their role as a security manager. These FSOs also develop security support teams to assist them in implementing their programs. Finally, the effective FSOs develop security education and training programs that provide employees with the knowledge and motivation for effective security performance. So what have we learned?

BEYOND COMPLIANCE MAKES SENSE

Compliance means meeting minimum requirements. FSOs said that an effective and efficient security program requires more than this. Excellence demands going beyond compliance. And this challenge means understanding customer and consumer needs, selling service and involving others in providing it.

Like other managers, FSOs have discovered that going beyond compliance makes sense. Quality assurance managers, for example, are improving quality and productivity by involving line personnel during production, rather than depending upon outside inspectors to identify defects after products are made. This integration of quality into the production function has significantly altered how quality managers operate and relate to other managers. Similarly, police departments are achieving greater control of crime through community policing. Community involvement has changed the way police officials assess problems and set priorities. Both of these examples reinforce what many FSOs have learned through experience: effective security programs require going beyond compliance. And this requires new ways of managing.

SECURITY EXCELLENCE DEMANDS LEADERSHIP

Leadership is vital for achieving security excellence. The FSOs readily acknowledged the importance of the many roles they were called upon to play. Some spoke of the role of security officer as one chiefly involved in enforcement or compliance aspects of their jobs. All referred to their responsibilities as managers in bringing about effective programs. But when asked to talk about what they did, how they did it and why, they spoke principally about leadership. Several used the metaphor of coach: developing the talent around them, helping people to perform better, empowering people, and guiding and nurturing staff and other employees in achieving security objectives.

The FSOs used leadership skills to sell and maintain their security programs. Effective

leadership enabled them to meet the sometimes conflicting requirements of their numerous customers. Without such leadership, key ingredients such as management support, employee involvement, and getting close to the consumer, become meaningless.

FSOs FACE DEMANDING CHANGES

Yogi Berra has been credited with the following observation: "The future just ain't what it used to be." Yogi's logic captures an idea that is central to future security programs. The hidden wisdom of his words is that change, and the challenge that it represents, is a constant companion of the manager. Deborah Collins, current president of the NCMS, recently cited several changes facing government security professionals:

* Tougher customer inspections
* Tougher sanctions for failed inspections
* Enhanced cooperation with good contractors
* More stand-alone security systems
* More security personnel to meet customer requirements
* More emphasis on reinvestigations for cleared personnel
* Increased emphasis on sophisticated security awareness training

Likewise, expected defense budget cuts, demands for increased productivity, increasing organizational complexity, and technological advances pose challenges for all managers. There will be greater emphasis on productivity, quality, and accountability. Businesses will have to be more competitive. In the future, FSOs are going to face increasing demands by their companies and their profession for higher levels of performance. Excellent FSOs got to be excellent at least partly because they have already identified many of these challenges and have begun to respond.

If change is the challenge, then leadership is one of the answers. Security professionals who emulate the behavior and management philosophy of the FSOs we have described will have positioned themselves to adjust to the changes already taking place. Better yet, they will no doubt be responsible for helping to define and achieve new levels of security excellence in the future.

REFERENCES

Bennis, W., & Nanus, B. (1985). *Leaders*. New York: Harper & Row.

Grau, J. A. (1989). Selling security. *Security Awareness Bulletin (2)*, 1-13.

Hall, J. (1988). *The competence connection: A blueprint for excellence*. The Woodlands, TX: Woodstead Press.

Kouzes, J. M., & Posner, B. Z. (1987). *The leadership challenge: How to get extraordinary things done in organizations*. San Francisco: Jossey-Bass.

McClelland, D. C., & Burnham, D. H. (1976, March-April). Power is the great motivator. *Harvard Business Review*, 100-110.

National Classification Management Society. (1989). *DD 254 Handbook*. Rockville, MD: Author.

Peters, T., & Waterman, R. (1982). *In search of excellence*. New York: Harper & Row.

REPORT EVALUATION FORM

We would like your feedback concerning the readability of this report and the expected usefulness of the information to you in your job. Please place your ratings in the spaces provided. Assign ratings as follows: A for excellent, B for above average, C for average, D for below average, and F for unsatisfactory. Send the form to:

Defense Personnel Security Research and Education Center
99 Pacific Street Suite 455-E (Code KC)
Monterey, California 93940-2481

1. Evaluation Ratings

   _____Readability of report

   _____Usefulness of information

   _____Overall grade

2. I am a: (check one of the following)

   _____Government/Military Security Manager

   _____Defense Industrial Security Manager

   _____Other (list job title)_____

3. Comments/Suggestions (use other side if necessary)

☆U.S. GOVERNMENT PRINTING OFFICE: 1995 - 628-087/26083